BEFORE
THE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET
UNITED STATES HOUSE OF REPRESENTATIVES

DELETING ONLINE PREDATORS ACT OF 2006

JULY 11, 2006
WRITTEN TESTIMONY OF
TED DAVIS
FAIRFAX COUNTY PUBLIC SCHOOLS

Thank you Chairman Upton and members of the Subcommittee for this opportunity to testify on the Deleting Online Predators Act of 2006.

My name is Ted Davis and I am an information technology director with Fairfax County Public Schools (FCPS) in Virginia. FCPS is the 14th largest public school district in the United States with over 163,000 students at 228 schools. FCPS long ago recognized the promise of the Internet as an educational resource, as well as its perils. Thus, in 1997, I was tasked with leading the effort to develop our Internet use policy and to implement filtering technology. FCPS supports the goals of the proposed legislation, but opposes the legislation in its current form. As I will elaborate, public schools are addressing the dangers of online predators, the legislation would not substantially improve the safety of our students, and it will place an added burden on schools.

Based on input gathered from nearly 800 educators, students, parents, and community members, we recognized that technology alone could not address our shared concerns for the safety of our students. Thus in 1998 the Fairfax County School Board adopted a policy that emphasized education, classroom management, personal responsibility, as well as technology.

Two years prior to the Children's Internet Protection Act of 2000, FCPS implemented a filtering technology now known as Symantec Web Security (SWS). FCPS filters web content that is obscene, harmful to juveniles, child pornography, and promotes illegal activities. Today, all 90,000+ of our computers are filtered for such content.

SWS enables school districts to select from a wide range of categories of inappropriate materials for filtering, such as sex, crime, violence, intolerance, and interactive chat, so that districts may select materials to be blocked based on their policies. As you know, the Internet is constantly changing, thus filtering vendors, like Symantec, continually update their lists of inappropriate web sites in these categories. Filtering vendors use a combination of technology and human review to identify and classify inappropriate web sites.

Furthermore, SWS provides school districts the ability to block (or unblock) additional sites in accordance with the needs of the school system. FCPS put into place a process and guidelines for identifying and evaluating web sites for possible filtering. Social sites, like MySpace.com, fell under this process. In the case of MySpace.com, FCPS began blocking this site last November. The same is true for many sites that preceded the popularity of MySpace.com. Neighboring school districts took similar actions—much to the relief of parents and dismay of students.

As you might expect, there will always be some determined students that seek to bypass technology protection measures—these students are subject to policy enforcement. Each school year FCPS students and their parents are required to sign our Acceptable Use Policy, which outlines appropriate and inappropriate uses of computers and the Internet. Failure to comply with this policy results in disciplinary action. Fortunately, this is not a significant problem. In this past school year 578 students were disciplined for violating our Acceptable Use Policy—representing 0.3% of our student population.

One strategy for deterring AUP infractions is through good classroom management. That is how teachers make use of the Internet in their classrooms. This includes approaches such as arranging computers so that screens are visible to the teacher, pre-selecting web sites for instruction, walking the classroom, and interacting with students as they use the web. FCPS teachers are trained to work these practices into their technology routine.

Technology measures, policy enforcement, and classroom management are good strategies for preventing access to inappropriate materials in school, but they do not sufficiently prepare our students to deal with potential dangers outside of school—at home, a friend's house, a coffee shop—or even when they become adults. We know that our students will need to deal with many dangers—not only sexual predators, but also identity thieves, scams, phishing schemes, viruses, deceptive advertising, and misinformation. Education is the key to preparing our students to deal with these dangers.

That is why FCPS begins at the earliest age to teach students how to take advantage of the Internet and to deal with its dangers. We teach them not to give out personal information, that people may not be who they say they are, and never to agree to meet someone via the Internet. To make our point, we also partner with the Fairfax County Police who can speak to our students of these dangers from real experience.

Parents are also key to protecting and educating their children. To help parents, we conduct cyber safety nights to educate them on the benefits and dangers. We teach parents to get involved in their children's Internet use at an early age, to set rules on Internet use, and to place computers with Internet access in a common area of their homes. We also reach out to busy parents via brochures and videos.

The strategies I described, taken together, have been effective in FCPS for many years now. These strategies are not the direct result of state or federal legislation. Rather, they are the result of the close relationship our schools enjoy with our students, parents, and community—and our shared passion to provide a safe learning experience that meets our students' needs.

Nevertheless, since the passage of the Children's Internet Protection Act six years ago, these strategies are now commonplace in school districts throughout the country.

The proposed legislation, though an extension of similar provisions in effect today, does not lend itself to a technical solution. It would require that schools block commercial social networking sites that “may easily be” misused to perpetrate inappropriate contact with students. Unlike current restrictions against obscene materials that can be objectively identified, this legislation would require schools to subjectively predict which sites may be misused. Identifying and evaluating such sites would not take advantage of the technical capabilities of filtering vendors and likely lead to blocking of legitimate instructional sites. Thus this burden would fall back on to the schools.

More could be done, of course. You can help protect our students by pursuing those individuals who would do harm to our children, and you can help us educate and prepare our students to be safe citizens of the Internet. To these ends, you could support law enforcement activities that seek to apprehend predators before they harm a child. You can facilitate collaboration between law enforcement agencies, filtering vendors, and schools to share information on web sites used to commit crimes; and you could foster an information campaign to reach parents and students on how to face the dangers on the Internet.

Thank you again for this opportunity to speak before the committee. I welcome your questions.

BEFORE
THE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON TELECOMMUNICATIONS AND THE INTERNET
UNITED STATES HOUSE OF REPRESENTATIVES

DELETING ONLINE PREDATORS ACT OF 2006

JULY 11, 2006
SUMMARY OF WRITTEN TESTIMONY OF
TED DAVIS
FAIRFAX COUNTY PUBLIC SCHOOLS

Background:

- Ted Davis is an information technology director at Fairfax County Public Schools (FCPS) that led the development of the FCPS Internet use policy and filtering technology implementation.
- FCPS is the 14th largest public school district in the United States.
- FCPS supports the goals of the legislation, but opposes the legislation as written.

Protecting students on the Internet at FCPS:

- Internet use policy emphasizes education, classroom management, personal responsibility, as well as technology.
- Implemented the Symantec Web Security (SWS) product in 1998.
- Filters content based on pre-selected SWS categories.
- Established a process for filtering additional web sites.
- Began blocking MySpace.com in November, 2005.
- Enforces an Acceptable Use Policy to deter inappropriate behaviors.
- Performs classroom management activities to mitigate infractions of its policies.
- Technology measures, policy enforcement, and classroom management do not prevent inappropriate behaviors outside of the school.
- Education of students and parents is key to preparing children to deal with dangers on the Internet.

Legislation:

- The proposal to block social networking sites that “may easily be” misused does not lend itself to a technical solution.
- Identifying sites that may be misused is subjective and would place an added burden on schools.
- The Subcommittee could help schools by:
    - Supporting law enforcement in identifying and apprehending predators.
    - Facilitating collaboration between law enforcement agencies, filtering vendors, and schools in identifying web sites used to commit crimes.
    - Fostering an information campaign to reach parents and students on how to face dangers on the Internet.